IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ACCOUNTS THAT ARE STORED AT PREMISES CONTROLLED BY YAHOO | Magistrate No. 16-699M **[UNDER SEAL]** |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Aaron O. Francis, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Yahoo, an email provider headquartered at 701 First Avenue, Sunnyvale, CA 94089. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3. I have been a Special Agent with the Federal Bureau of Investigation (FBI) for six years. During that time, I have received training in computer crime investigations. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search and seizure warrants, and the identification and collection of computer-related evidence. I am currently assigned to the Pittsburgh Division Cyber Intrusion Squad.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 371 (Conspiracy), 1030(a)(4) (Unauthorized Access of a Protected Computer in Furtherance of Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire/Bank Fraud), and 1956 (Laundering of Monetary Instruments) (hereinafter the "Target Offenses") have been committed by as yet unknown persons in control of an email account (hereinafter the "Target Account") described below. There is also probable cause to search the Target Account described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes, and identification of those committing these crimes, further described in Attachment B.

## JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## EXPLANATION OF RELEVANT TERMS AND CONCEPTS

7. "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers' computers. ISP's typically log their customers' connections, which means that the ISP can identify which of their customers was assigned a specific IP address during a particular session.

8. "Server" is a centralized computer that provides services for other computers connected to it through a network. The computers that use the server's services are sometimes called "clients." Server computers can be physically located anywhere. For example, it is not uncommon for a network's server to be located hundreds, or even thousands, of miles away from the client computers.

9. "Emails" sent over the internet contain IP addresses that can be used to determine the origin and destination of the message. The "header" of an email, which is attached to the top of every email and contains IP addresses of computers which have transmitted the email, may be used to identify the "path" through the internet the email traveled from its origin to its destination. The header will often contain the IP addresses of any and all servers from which the given email "bounced" en route to its destination. These IP addresses may be traced to determine the sender of a specific email. The header will also contain the email address(es) that the message was sent to and the email address that the message was sent from. Based on my

training and experience, I know that email accounts are one of the predominant ways in which individuals communicate privately over the Internet. Furthermore, I know that email accounts very often contain communications and/or other information which can be used to identify the user of the accounts and their physical location. Such information is critical in determining the true identity of members, their location, and the extent of their criminal activities.

10. Business Email Compromise (BEC) scam is a scheme designed to target businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

## YAHOO EMAIL AND RELATED SERVICES

11. This affidavit is made in support of an application for a search warrant pertaining to a certain email account and related Yahoo services provided by the web-based electronic mail and remote computing service provider known as Yahoo. The account (hereinafter referred to as the "Target Account") to be searched is:

**adegebo@yahoo.com**

12. The Target Account is a Yahoo email account. In my training and experience, I have learned that Yahoo provides a variety of online services, including electronic mail access, to the public. Yahoo allows subscribers to obtain email accounts at the domain name yahoo.com like the Target Account listed in Attachment A. Subscribers obtain an account by registering with Yahoo (Provider). During the registration process, Provider asks subscribers to provide basic personal information. Therefore, the computers of Yahoo are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo subscribers) and information concerning subscribers and their use of services, such as account access

information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In general, I know that an email that is sent to a Yahoo subscriber is stored in the subscriber's "mail box" on Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Provider's servers for a certain period of time.

13. A Yahoo subscriber can also store with the Provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the Provider. In addition, subscribers to these accounts may enlist other internet services that are associated with the account. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, attachments to emails, including pictures and files.

## INVESTIGATIVE RELEVANCE OF EMAIL ACCOUNT SERVICES

14. In my training and experience, subscriber information collected by service providers may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

15. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This

information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

16. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of

occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Lastly, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

18. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Yahoo (i.e., the "Provider") may not be. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. Yahoo employees may not be. It would be inappropriate and impractical, however, for federal agents to search the vast computer networks of Yahoo for

the relevant accounts and then to analyze the contents of those accounts on the premises of Yahoo. The impact on Yahoo's business would be severe.

19. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Yahoo, to protect the rights of the subjects of the investigation and to effectively pursue this investigation, authority is sought to allow Yahoo to make a digital copy of the entire contents of the information subject to search specified in Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Attachment B.

20. Executing a warrant to search Yahoo email accounts requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject email account in this case for evidence of the target crimes will require that agents cursorily inspect all emails produced by Yahoo in order to ascertain which contain evidence of those crimes, just as it is necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to ensure that law enforcement can discover all information subject to seizure pursuant to Attachment B. Keywords search text, but many common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

## PROBABLE CAUSE

21. On February 12, 2016, the FBI-Pittsburgh Office was notified that OSF St. Francis Inc. (OSF), a company headquartered in Peoria, Illinois, had been the victim of a

Business Email Compromise (BEC) scam that resulted in the issuance of a fraudulent wire transfer in the sum of $150,000 (USD), from PNC Bank, a Pittsburgh-based bank, to Woori Bank located in South Korea.

22. OSF employee, Steve Coughlon, was interviewed by the FBI. According to Coughlon, on February 12, 2016, he received a series of emails purporting to be from OSF President, Kevin Schoeplein. The emails were received by Coughlon at his email address of steve.m.coughlon@osfhealthcare.org and appeared to be from Kevin Shoeplein. The emails instructed Coughlon to wire $150,000 (USD) to Woori Bank located in South Korea to a beneficiary by the name of "Adewale Hakeem Aliu." Coughlon followed the instructions in the emails and initiated the wire transfer.

23. Upon completing the wire transfer, Coughlon provided the wire details to another employee, Richard Haney, believing that the PNC Bank would contact Haney to verify the details of the wire. According to Coughlon, Haney advised that the "mailto" address was not Schoeplein's email address but instead was and email account identified as praveen.zaman67@gmail.com. Coughlon immediately notified the PNC Bank and attempts were made to recall the wire transfer.

24. Later that same day, the PNC bank notified the FBI of the attempted fraudulent wire transfer. At the FBI's request, the Korean National Police Agency (KNPA) arranged to freeze and flag the Woori Bank account associated with the receipt of the wire transfer.

25. On February 16, 2016, your affiant participated in a conference call with FBI and KNPA officials. KNPA Senior Inspector Jeremy Kim advised that earlier that day (i.e., February 16th) at approximately 11:20 am (Seoul, South Korea Time), KNPA officials arrested Femi David Gbolade, Jamiu Opeyemi Fatai, and Hakeem Aliu Adewale, as they attempted to

withdraw the fraudulent funds from the frozen Woori Bank account.

26. According to KNPA officials, seized during the arrest of Adewale was a fraudulent invoice for a $150,000 (USD) wire transfer, along with a fraudulent purchase agreement and a wire receipt in the name of OSF, the victim company. KNPA officials interviewed all three subjects. Information provided by Fatai revealed that he was to receive 5% of the $150,000 (USD) and Adewale would receive 15% of the $150,000 (USD) for their participation in the scheme. According to KNPA officials, Fatai believed the fake invoice found on Adwale had been emailed to Gbolade by Rasaq Bola Hameed utilizing the email account ayinkequadir@gmail.com. Fatai further identified the email account sheuq48@gmail.com as the account from which he believed Hameed sent him (Fatai) an email regarding the location of the bank from which the funds were to be withdrawn.

27. The FBI examined the emails received by Coughlon that purported to be from Schoeplein. An examination of the headers associated with those emails revealed that the emails were actually sent from praveen.zaman67@gmail.com. Additionally, the headers associated with the emails showed that Coughlon's reply emails were directed to praveen.zaman67@gmail.com.

28. KNPA officials also searched Gbolade's residence, which he shared with Hameed. During the search they recovered fake invoices, computers, and phones.

29. On March 3, 2016, the FBI executed a search warrant on Google for the contents of the email account sheuq48@gmail.com, the account identified by Fatai to KNPA officials.

30. The search of the contents of the account revealed that on February 3, 2016, sheuq48@gmail.com sent an email to romeonkevin@yahoo.com. The email contained a fake purchase agreement between Rockfarm Logistics, LLC (Rockfarm) and Baysah Abel Trokon, in

the amount of $150,000. Significantly, during the February 16, 2016 search of the residence shared by Gbolade and Hameed, KNPA officials discovered a bank transaction receipt in the amount of $150,000 and the sender of the wire was identified as "Rockfarm."

31. FBI Agents interviewed an employee of Rockfarm. This employee stated that Rockfarm did initiate a wire transaction to Trokon and the transaction was initiated as the result of a BEC scam. Rockfarm attempted to have the transaction recalled but they were unsuccessful and suffered a loss of $150,000.

32. The search of the contents of the sheuq48@gmail.com account also revealed that on February 15, 2016, sheuq48@gmail.com sent an email to femidear@yahoo.com. The email contained a wire transaction receipt for $150,000 dated February 12, 2016. The beneficiary of the wire was Adewale and the beneficiary account number was listed as "x5950." As explained above, Adewale was arrested by KNPA officials on February 16, 2016 attempting to withdraw $150,000 from Woori Bank. Additionally, the victim (OSF) was directed to wire $150,000 to a Woori Bank account ending in 5950.

33. Subscriber data received from Google revealed that the phone number listed for sheuq48@gmail.com was +2348062976426. Significantly, during the search of phones seized from Gbolade, KNPA officials discovered that on February 11, 2016, an individual utilizing phone number +2348062976426 sent two fake invoices to Gbolade via WhatsApp, an instant messaging application that allows certain smartphone users to exchange text, image, video, and audio messages.

34. Additional subscriber data received from Google further revealed that the recovery email address for sheuq48@gmail.com was aluko667@gmail.com. On May 4, 2016, the FBI executed a search warrant on Google for the contents of aluko667@gmail.com.

35. The search of the contents of the account revealed that on December 31, 2012, aluko667@gmail.com received an email from Google advising that the account sheuq48@gmail.com had been created.

36. The aforementioned searches of the contents of both the sheuq48@gmail.com and aluko667@gmail.com email accounts revealed that on June 16, 2013, the Target Account adegebo@yahoo.com sent the exact same email to both the sheuq48@gmail.com and aluko667@gmail.com email accounts. Both emails were sent approximately five minutes apart and contained the text "my pp." Both emails contained a passport for Ajibola Dolalekan Bello Aluko, DOB 11/07/1961, Passport Number A02671900.

37. Subscriber data provided by Google revealed that the recovery email address for aluko667@gmail.com was Target Account adegebo@yahoo.com.

38. Based on open source searches, I learned that Target Account adegebo@yahoo.com was used to register multiple social media accounts, including Facebook account wale.adegebo. The profile photograph on Facebook account wale.adegebo, the passport photograph on Aluko's passport (referenced above), and multiple "selfie-style" photographs contained in the Google data for aluko667@gmail.com are of the same person.

39. All the emails from adegebo@yahoo.com contained in the Google data for aluko667@gmail.com contain the "from line" of "Adewale Adegebo <adegebo@yahoo.com>."

40. On July 22, 2014, Target Account adegebo@yahoo.com sent an email to aluko667@gmail.com containing one attachment. The attachment was a resume for Mrs. Hidayat Wale Adegebo. Significantly, this shows that it is likely that identity evidence is likely to be obtained from the search of the Target Account.

41. Google data for aluko667@gmail.com contained photographs of bank deposit

slips for First Bank of Nigeria in the name Adewale Adegebo,

42. Based on the above, my knowledge of this investigation, and my training and experience, I have probable cause to believe that the user of sheuq48@gmail.com, aluko667@gmail.com and the user of Target Account adegebo@yahoo.com are the same person, and that evidence of the Target Offenses, including the identities of the perpetrators, are likely to be found within the Target Account.

## CONCLUSION

43. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant. Because the warrant will be served on Yahoo who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Aaron O. Francis, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 20th day of July, 2016

HONORABLE MAUREEN P. KELLY
CHIEF UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT A

**Property to Be Searched**

This warrant applies to information associated with email account:

adegebo@yahoo.com

that are stored at premises controlled by Yahoo, a company that accepts service of legal process at 701 First Avenue, Sunnyvale, CA 94089.

## ATTACHMENT B

### Particular Things to be Seized

### I. Information to be disclosed by Yahoo (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the Target Account listed in Attachment A, from inception of the account to the present:

a. The contents of all emails and communications associated with the Target Account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. Web history files or documents pertaining to historical searches performed by the user.

c. Files and/or documents pertaining to any Android Devices, Android Market, and Location History.

d. All other communications and messages made or received by the user, including all private messages, chat history, and video calling history.

e. All location information.

f. All IP logs, including all records of the IP addresses that logged into the Target Account.

g. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session

times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

h. Any accounts associated with the Target Account by recovery email, secondary email, SMS recovery number, cookie data; and/or overlapping logins by users with a common IP address;

i. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

j. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

## II. Particular Things to be Seized by the Government

All evidence and information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of the Target Offenses, namely, violations of Title 18, United States Code, Sections 371 (Conspiracy), 1030(a)(4) (Unauthorized Access of a Protected Computer in Furtherance of Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud) 1349 (Conspiracy to Commit Wire/Bank Fraud) and 1956 (Laundering of Monetary Instruments), from inception of the account to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. The content of any and all electronic communication, and any internet search history, other internet activity, or documents, that pertains to:

   a. The identity of the user(s) of the Target Account, to include (but not limited to) names, location of the user, passwords, IP addresses, email communications with other internet accounts (whether email, domain, or any other) under the control of the user(s).

   b. Evidence pertaining to obtaining unauthorized access to others' computers,

particularly through the usage of spoofed, re-routed or fraudulent emails;

c. Evidence indicating how and when the email accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account users;

d. Evidence indicating the email accounts' user's state of mind as it relates to the crimes under investigation;

e. The identities of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

f. The identity of the person(s) who communicated with the account about matters relating to the Target Offenses including records that help reveal their whereabouts;

g. Business Email Compromise Activity relating to the Target Offenses in all of its forms, including but not limited to the identification of victims; communications with victims/co-conspirators/accomplices; the use of bank accounts to receive funds acquired by the fraudulent activities; the creation of fraudulent invoices; and the creation/use of email accounts and other online services in furtherance of the criminal activities;

h. Motive for computer intrusion and fraudulent business email compromise activity;

i. The illegal trafficking of personal identifying information, usernames and passwords of compromised computers or internet accounts, or any other items which are being offered, requested, or possessed without the authorization of the bona fide owner;

**2.** Any and all records or other information pertaining to the identity of the subscriber of the Target Accounts, including but not limited to associated email accounts, login IP addresses, and session times and durations.